UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
NORTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case Number 06-20657-BC
Honorable Thomas L. Ludington

CRAIG A. ROBSON,

Defendant.
_____ /

ORDER DENYING IN PART DEFENDANT'S MOTION TO SUPPRESS EVIDENCE AND SCHEDULING ADDITIONAL HEARING ON THE MOTION

On January 10, 2007, a federal grand jury returned an indictment, charging Defendant Craig Robson with seven counts of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2)(B); one count of using a computer to distribute lewd or lascivious content, in violation of 18 U.S.C. § 1465; and one count of using the internet to solicit a minor to engage in sexual activity, in violation of 18 U.S.C. § 2422(b).

On May 24, 2007, Defendant filed a motion to suppress evidence obtained from his mother's computer, as seized in violation of the Fourth Amendment. On July 16, 2007, the Court held a hearing on that motion to suppress and received testimony from three witnesses. Based on their testimony and Defendant's exhibit of a police report of September 11, 2006 of three interviews of witnesses, the Court finds the following in summary of the relevant events.

Defendant's mother, Ms. Sandra Robson, testified that her son periodically stayed overnight at her apartment, often in advance of appointments he had on Fridays. She slept in the apartment's single bedroom, and he would sleep on a sofa-sleeper in the living room. Defendant's mother owned

the personal computer at issue, which she received as a gift from a former tenant in the building. She kept the computer in her living room. She is the lessee of the apartment. Defendant's mother is also exclusively responsible for the telephone account and the internet service provider account. Because she did not wish to miss any phone calls and because her internet access required modem access to her phone line, she did not permit Defendant to use the computer until after she retired for the evening, around 9 or 10 p.m. She did, however, allow her son to use her computer. According to her first interview with a police officer, Defendant was previously convicted for delivery of child pornography.[1] Although it received passing attention during Defendant's mother's testimony, she did suggest that she would not have permitted her son to use the computer to access pornography.

The computer login screen listed two icons to access two user profiles, one for herself and one for her son. Accessing each user profile required a password. She did not have her son's password, and he did not have her password. She acknowledged that, at several points in time, she tried to monitor her son's use of the computer. She did not succeed in doing so because she lacked her son's password.

Around September 9, 2006, she received a phone call from Katrina Rose Garret, her son's child's mother. The woman related that she had found child pornography on her computer after a visit from Defendant. Defendant's mother then spent three hours one night and three hours the next morning attempting to identify whether any such material was also stored on her own computer. She testified that she used a search utility which allowed her to select all files or folders. Although her searches initially generated no results, when she searched on the term "trash," she located at least two files that contained that term. In her assessment, the location containing those files appeared

[1]Dft. Ex. 1, p. 1.

to contain all the image files ever stored on the computer. Indeed, she noted that many of the images were photos stored on the computer by its prior owner. She found these files without needing to use her son's password. Of the two files identified by her search, one file contained an image of a twelve or thirteen-year-old girl lying on her side, and the other file contained an image of two naked boys. In Defendant's mother's view, these images were child pornography. She described her response to discovering these images as "hysterical." Had her son been present at that time, she stated that she would have assaulted him.

She then contacted the Federal Bureau of Investigation (FBI), and at their suggestion, contacted her local police department. Defendant's mother testified that a police officer came to her home on September 10, 2006 and, with her consent but without a warrant, took the central processing unit of her computer (i.e., the tower), which contained the hard drive.

During the hearing, counsel stipulated to the admission of three Bay City police reports. An Officer Querback prepared each of the reports on September 11, 2006. The reports memorialized three interviews: (1) a conversation with Defendant's mother at her apartment on September 10, 2006 when she surrendered her computer to a Bay City police officer as evidence; (2) a telephonic interview on September 11, 2006 with the mother of Defendant's child, in which the report recites that "Corporal Petro went to [her] residence and seized her computer tower"; and (3) a telephonic interview on September 11, 2006 with Defendant's mother. *See* Dft. Ex. 1. Defendant's mother testified that, during her first interview, she showed the officer what she found and described how she found it. She believed that she was "divulging everything he could possibly want." She also recalled explaining that she did not have access to his Yahoo! e-mail account, as she did not have his password. Although she did not then tell the officer about any password protection on her son's

user profile, she later related to the officer during the interview on September 11, 2006, that she did not have the password to access Defendant's user profile on her computer. Dft. Ex. 1, p. 3. The interview summary, however, is unclear as to whether she was referring to the password for his user profile or the password to his internet service provider account.

Special Agent Banner of the FBI, the co-case agent, testified next. He explained that Defendant's mother was interviewed by the FBI on October 10, 2006 by his co-case agent and after she had surrendered her computer. He testified that, sometime in October 2006, the FBI obtained the computer from the Bay City police department and then submitted it for examination to an FBI forensic examiner. In December 2006, when Agent Banner had his first contact with Defendant's mother and after the forensic examination of the computer, he had no need to ask her for any password. The forensic examiner, Banner explained, had the technical means to bypass the password protection created by Defendant.

Mr. Walker Sharp, a member of the Computer Analysis Response Team of the FBI, performed the computer forensic examination. He testified during the hearing without the benefit of his file or report. He could not recall when he received Defendant's mother's computer. He examined the hard drive and did not review any other source of information about the case or any other information about the location where images might be stored. Using forensic tools, he identified the files on the hard drive. Each file contained a creation date, which reflects when that file was first stored in that location on the computer. He identified several hundred images on the hard drive that he believed could constitute child pornography that were downloaded at three or four specific times.

Some of the files identified by the forensic examiner, which he theorized were probably the

files viewed by Defendant's mother, were located in a "deleted" but shared space. That is, those files were stored in a location unassociated with a particular user profile, while most of the other files of interest were located in storage space specific to Defendant's user profile. Sharp explained that the operation of his forensics tool allowed him to bypass password protection at the user profile level but that, by the end of his protocol, he could identify the images subject to the password protection of Defendant's user profile. No files or folders were encrypted.

Without access to his report, Sharp could not testify which of the images (that serve as the basis of seven counts in the indictment) were stored under Defendant's user profile and which were stored in shared space, unassociated with any particular user profile. Sharp did state, however, that he could review his "media findings report" to determine where particular files were located. In addition, he used a forensic tool to save an image of the entire hard drive. The parties reserved the opportunity to advance additional proofs, depending on the Court's resolution of the issue of Defendant's standing to challenge the government's search of his mother's computer.

Defendant alleges that his mother's surrender of her computer to authorities and her consent to search the computer's hard drive did not authorize them to search files accessible only through his user profile. He contends, without objection, that he and his mother mutually respected each other's privacy through their mutual use of password protection. Defendant concedes that his mother owned the computer, so the government challenges Defendant's standing to object to the search of the hard drive.

Fourth Amendment rights are personal and may not be vicariously asserted. *Rakas v. Illinois*, 439 U.S. 128, 133-134 (1978) (citations omitted). "A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third

person's premises or property has not had any of his Fourth Amendment rights infringed." *Id*. at 134 (citation omitted). Additionally, a search by a private party – without government action – does not violate a person's Fourth Amendment rights. *See United States v. Jacobsen*, 466 U.S. 109, 117-118 (1984); *United States v. Morgan*, 744 F.2d 1215, 1218-1219 (6th Cir. 1984) (noting that the Fourth Amendment proscribes only governmental action and not private individuals' actions, even if wrongful).

Here, Defendant has no standing to object to the use of the particular images located by his mother's search of her own computer without any knowledge or use of his password. Because Fourth Amendment rights are personal and cannot be vicariously asserted, Defendant cannot object to any potential violation of his mother's rights. Additionally, even if he had such standing, his mother's search constitutes a private search. No evidence suggests that Defendant's mother acted as an agent of the police. Rather, she acted on her own initiative and with unquestioned ownership and authority over the computer. Consequently, her search and any files that she identified from that search produce no Fourth Amendment violation as to Defendant. Files that she identified, thus, will not be excluded as the product of an improper search and seizure.

According to the government, however, it will rely on numerous files identified by the forensic examiner but not accessed by Defendant's mother. Defendant suggests that his use of a password for his user profile, as well as he and his mother's understanding of the privacy of each other's materials stored on the computer, show that he had a reasonable expectation of privacy in the files subject to the password that protected his user profile.

In order for a Fourth Amendment violation to occur, a person must have an actual subjective expectation of privacy and that expectation must be one that society is willing to acknowledge as

reasonable. *Katz v. United States*, 389 U.S. 347, 362 (1967) (Harlan, J., concurring); *see also Guest v. Lies*, 255 F.3d 325, 333 (6th Cir. 2001) ("[A] person must have had a subjective expectation of privacy in the place or property to be searched which was objectively reasonable.") (citation omitted).[2]

Courts have considered certain factors particularly relevant in assessing the reasonableness of an expectation of privacy. These factors include the following: (1) although not dispositive, the existence of a proprietary or possessory interest in item seized; (2) the defendant's right to exclude others from that item; (3) whether normal precautions were taken to maintain privacy; (4) whether the defendant had the subjective intention to be free from governmental intrusion; and (5) whether the defendant was legitimately on the premises. *United States v. King*, 227 F.3d 732, 744 (6th Cir. 2000) (citations omitted). Notably, a reasonable expectation of privacy, such as that of "[a] burglar plying his trade in a summer cabin during the off season," may well differ from an expectation that society and the law recognize as legitimate. *Rakas*, 439 U.S. at 143 n.12 (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).[3]

---

[2]"Although raised as an issue of 'standing,' the question of whether a defendant may contest an allegedly illegal search collapses into the substantive issue of whether the defendant had a legitimate expectation of privacy. . . . If there is no legitimate expectation of privacy, it adds nothing to say that the defendant had 'no standing.'" *United States v. McRae*, 156 F.3d 708, 710 n.1 (6th Cir. 1998) (citations and internal quotations omitted).

[3]The government notes that the Supreme Court in *Rawlings v. Kentucky*, 448 U.S. 98, 106 (1980), stated that a defendant had no legitimate expectation of privacy for drugs he had placed in another person's purse. While technically correct, the Court's analysis there involved several other significant factors. These included the following: (1) the purse owner's statement that she had only known the defendant for a few days; (2) the defendant had never previously accessed her purse; (3) the defendant had no right to exclude others from her purse; (4) the defendant placed items in her purse only a short time before the police arrived; and (5) the defendant admitted that he had no subjective expectation of privacy in her purse. Accordingly, the *Rawlings* decision exemplifies the fact-specific inquiry necessary to determine whether a legitimate expectation of privacy exists, rather

Here, unlike a burglar in a cabin, Defendant's use of the computer occurred with the consent of the computer owner. Although his mother had a visceral response to seeing particular images that Defendant stored on the computer, his presence on the computer occurred with his mother's consent. Indeed, she did not withdraw her consent, even after she had suspicions that he might have disregarded her preferences.

As to other factors, Defendant lacked a possessory interest in the computer, but he did have a possessory interest in files stored under his user profile on that computer. Also, his use of a password to protect his user profile shows his right to exclude others from accessing those files, even if such a password would not necessarily prevent access to the hard drive through the use of specialized forensic software. Similarly, his mother did not share her password with him, suggesting that he had a corresponding inability to access files stored under her user profile. The possibility that other mechanisms might have sufficed to evade the password requirement, such as the forensic protocol employed by the FBI's examiner or greater technical expertise than possessed by an average computer user, underscore that Defendant took normal precautions to maintain privacy for the contents under his user profile.

As to any subjective intention to be free from governmental intrusion, Defendant offered no evidence of his own state of mind, other than his use of a password, but that bespeaks a generalized preference to be free from intrusion, regardless of its source. Finally, as discussed previously, Defendant's mother's consent to his use shows that he was legitimately on the "premises." Thus, the Court concludes that Defendant had a subjective expectation, which society would treat as objectively reasonable, in the privacy of files stored on his mother's computer, to the extent that

---

than a narrow proposition regarding contraband hidden in another person's property.

those files were generally accessible only through his password-protected user profile.

The existence of a reasonable expectation of privacy, however, does not resolve the issue. Defendant's mother contacted the authorities, showed them the files she identified, consented to surrender her computer, and turned over to them with the central processing unit that housed the hard drive.

Even without a warrant or probable cause, a search is permissible under the Fourth Amendment with valid consent. *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) (citations omitted). The common authority that justifies a search based on third-party consent "rests . . . on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched." *United States v. Matlock*, 415 U.S. 164, 171 n.7 (1974) (citations omitted). If the prosecution relies on consent as the basis for the legitimacy of a search, then the government must show that consent was freely and voluntarily given. *Schneckloth*, 412 U.S. at 222. Similarly, the government bears the burden to show that a third party had authority to consent to a search. *United States v. Arnold*, 486 F.3d 177, 213 (6th Cir. 2007) (citing *Illinois v. Rodriguez*, 497 U.S. 177, 181 (1990)).

The scope of the consent is constrained by the bounds of objective reasonableness, based on the consenting person's exchange with the officer. *Florida v. Jimeno*, 500 U.S. 248, 251 (1991). Also, if a third party without actual authority but who the police in good faith believe has that authority, then no Fourth Amendment violation occurs if the police rely on that apparent authority to conduct a search. *United States v. Morgan*, 435 F.3d 660, 663 (6th Cir. 2006) (citing the objective

standard of whether "officers reasonably could conclude from the facts available that the third party had authority to consent to the search") (citations and internal quotations omitted). "If apparent authority existed at that time, later-discovered facts that might undermine the initial reasonable conclusion of third-party apparent authority are generally immaterial." *Id*. at 664.

In *Trulock v. Freeh*, 275 F.3d 391, 403-404 (4th Cir. 2001), the Fourth Circuit considered a case involving evidence found in files stored on a shared computer in the bedroom of a pair of co-workers and co-occupants of a home. The court held that one of the co-occupants had authority to consent to a general search of the computer, but the court held that that consent did not extend to the other person's password-protected files. *Id*. The court relied on an analogy to *United States v. Block*, 590 F.2d 535, 541 (4th Cir. 1978), in which a defendant's mother's consent to a search of his room in their home did not extend to consent to search a locked footlocker inside the defendant's room.

In an unpublished decision in *United States v. Aaron*, 33 Fed. Appx. 180 (6th Cir. 2002), the Sixth Circuit affirmed the district court's denial of a motion to suppress evidence of child pornography found on the defendant's computer. The defendant's live-in girlfriend authorized the police to search the home (which she owned), and there was no evidence that the defendant limited her access to his computer, either through technical means or because of his directive. Reviewing the law regarding searches of containers in other circuits, the Court stated that courts generally consider the nature of the container at issue and any efforts to ensure privacy. *Id*. at 184. "In the personal computer context, courts examine whether the relevant files were password-protected or whether the defendant otherwise manifested an intention to restrict third-party access." *Id*. (citing *Trulock*, 275 F.3d at 403). Because the defendant had taken no affirmative step to prevent his

girlfriend's use of the computer, such as using password protection, the Court concluded that her consent was sufficient to permit the search of the computer. *See also Morgan*, 435 F.3d at 663-664 (holding that a wife's apparent authority over a computer to which she had complete access sufficed to justify a warrantless but consented-to search).[4]

Here, no one contests that Defendant's mother voluntarily surrendered her computer to the police. Nor is it contested that she had the authority to do so, as she owned the computer. On one hand, Defendant's mother may have had and certainly would have appeared to have actual authority over her own computer and its contents. Her surrender of the computer to the police could suggest a grant of total permission to review its contents. On the other hand, if she related to the police that password protection existed for Defendant's user profile, a proposition that is neither established nor contradicted by the police reports received into evidence, then the police would have been on notice of her lack of authority to search files subject to the password protection of his user profile. If she alerted the police to that limitation on her access, regardless of that fact that the FBI forensic examination protocol only reveals that information at the end of its analysis, then concluding that her authority extended to those files becomes unreasonable.

Given the insufficiency the factual development at the hearing on when or whether Defendant's mother told the authorities about the existence of any password protections used by her son, the Court will hold an additional hearing and take additional proofs on that point. The parties may also provide supplemental briefing, giving particular attention to the circumstances of Defendant's password-protected user profile and the circumstances of Defendant's mother's consent.

---

[4]A more recent Supreme Court decision, *Georgia v. Randolph*, 547 U.S. 103 (2006), holding that a physically present co-occupant who objects at the time can prevent a police search otherwise valid due to the consent of the other co-occupant of a premises, has no obvious application here.

Accordingly, it is **ORDERED** that Defendant's motion to suppress [dkt #19] is **DENIED IN PART**, as to files identified in the course of the search conducted by Defendant's mother.

It is further **ORDERED** that an additional hearing is **SCHEDULED** on Defendant's motion for **September 6, 2007** at 9:30 a.m. The parties shall file any supplemental briefs on or before **August 20, 2007**.

s/Thomas L. Ludington
THOMAS L. LUDINGTON
United States District Judge

Dated: July 24, 2007

PROOF OF SERVICE

The undersigned certifies that a copy of the foregoing order was served upon each attorney or party of record herein by electronic means or first class U.S. mail on July 24, 2007.

s/Tracy A. Jacobs
TRACY A. JACOBS